INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

REC'D 25 OCT 2004
WIPO PCT

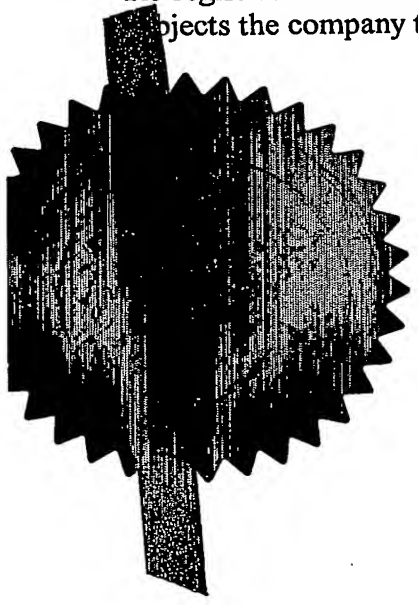
I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

I also certify that the attached copy of the request for grant of a Patent (Form 1/77) bears an amendment, effected by this office, following a request by the applicant and agreed to by the Comptroller-General.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.



Signed

Dated 11 October 2004

Patents Form 1/77

Patents Act 1977
(Rule 16)

The Patent Office

02OCT03 E941413-1 D03312
P01/7700 0.00-0322978.8

THE PATENT OFFICE
J
-1 OCT 2003
LONDON

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

1. Your reference GBP290028

2. Patent application number
(The Patent Office will fill in this part)

01 OCT 2003

0322978.8

3. Full name, address and postcode of the or of each applicant (underline all surnames)

Ver-Tec Security Systems Limited,
25 St Andrews Street
Cambridge
Cambridgeshire CB2 3AX
United Kingdom

8667263002

Patents ADP number (if you know it)

If the applicant is a corporate body, give the country/state of its incorporation

United Kingdom

4. Title of the invention

Data verification methods and apparatus

5. Name of your agent (if you have one)
"Address for service" in the United Kingdom to which all correspondence should be sent
(including the postcode)

~~Marks & Clerk~~
~~Wellington House~~
~~East Road~~
~~Cambridge CB1 1BH~~

Marks & Clerk
66/68 Hills Road
Cambridge
Cambridgeshire
CB2 1LA

Patents ADP number (if you know it)

~~18001~~

CAL-16.10.03

6. Priority: Complete this section if you are declaring priority from one or more earlier patent applications, filed in the last 12 months

Country	Priority application No (if you know it)	Date of filing (day / month / year)

7. Divisionals, etc: Complete this section only if this application is a divisional, application or resulted from an entitlement dispute

Number of earlier application	Date of filing (day / month / year)

8. Is a Patents Form 7/77 (Statement of inventorship and of right to grant of a patent) required in support of this request?

Yes

(Answer 'Yes' if:
a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

Patents Form 1/77

3. Accompanying documents: A patent application must include a description of the invention. Not counting duplicates, please enter the number of pages of each item accompanying this form:

Continuation sheets of this form	0
Description	11
Claim(s)	2
Abstract	1
Drawing(s)	5

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent (Patents Form 7/77)	
Request for preliminary examination and search (Patents Form 9/77)	
Request for substantive examination (Patents Form 10/77)	
Any other documents (please specify)	

11. I/We request the grant of a patent on the basis of this application.

Signature(s) Robert Clark. Date: 1 October 2003

12. Name and daytime telephone number of person to contact in the United Kingdom

Cambridge Office
01223 451038

TOTAL P.04

M&C Folio: GBP290028

Data Verification Methods and Apparatus

This invention generally relates to methods and apparatus for verifying data, and more particularly to holographic data carriers and apparatus for creating such data carriers, and to methods of verifying data stored on holographic data carriers.

Holograms are well known as security devices and biometric technologies are useful in verifying personal identity. Here a biometric comprises a human characteristic useful for identifying an individual, such as a fingerprint, face, iris or retina image, a voiceprint, and, of a more abstract nature, a pattern of finger lengths. It is noted that both a voiceprint and abstract characteristics such as finger patterns may be represented as an image.

Identity fraud (the use of a fraudulent identity) takes place in the context of drug running, money laundering, terrorism, fraudulent claiming, illegal immigration and, on a more personal level, credit card crime. The cost of such fraud is extremely high and standards are developing for machine-readable documents including a facial image and a contact-less integrated circuit chip encrypted using public key infrastructure technology. The chip may store images of a face (approximately 12k bytes when optimally compressed), a fingerprint (10k bytes) or an iris (30k bytes). There is, however, a continuing need for improved security, to stay at least one step ahead of counterfeiters.

Background prior art relating to holograms of fingerprints may be found in:

US 5,986,746; GB 2313944A; EP 0010611A; US 5,862,247; US 5,815,598; US 5,095,194; US 3,704,949; US 4,532,508; JP 63201795; JP 7096693A;

Therefore the invention provides, in a first aspect, a data carrier comprising: a hologram storing data to reproduce an image of a portion of a human body characteristic of an individual; and a second data bearing device; and wherein data stored by said second data bearing device is verifiable using data stored in said hologram.

In this way embodiments of the data carrier link the biometric image stored in the hologram to other data stored on the card so that this other data is verifiable using a hologram. The verification may be carried out using the holographically stored image itself or by employing additional information stored with the holographic image, for example in a different viewing plane. Thus the data stored by the second data-bearing device may comprise first data for verifying with the image – using either one of the first data and the reproduced image to verify the other – and second data which is in turn verified by this verification process.

Additionally or alternatively the hologram may store additional data such as a code, for example an alphanumeric code or a bar code. The data stored by the second data-bearing device may comprise third data for verification with this additional data (either one verifying the other) and fourth data verified by this verification process. The aforementioned second and fourth data may comprise the same data to, in effect, provide a double- or cross-check – for example the holographic image may be employed to verify data stored by the second data bearing device and, in turn, data stored within this device may be used to verify, say, a code stored within the hologram.

The hologram may store the image in a first view and the additional data in a second view, for example these views comprising different planes of a reproduced holographic image, preferably such that the image and the additional data are separable by a viewing system. Optionally a third view or image plane may store further additional data within the holograph such as, for example, an identifier for a machine which was used to record or fabricate a hologram.

Optionally the additional data and/or further additional data, that is views other than the reproduced image view, may be recorded at an angle or wavelength (for example in the

ultraviolet or infrared) such that reproduction at a wavelength visible to the human eye is inhibited.

Preferably the hologram comprises a reflection or volume hologram. Preferably the image comprises a substantially two-dimensional image to facilitate verification and, where employed, the storage of additional data. The second data bearing device may comprise an integrated circuit memory device such as a smart card chip, and is preferably tamper-resistant. However in other arrangements the second data bearing device may comprise a substrate bearing graphics, preferably machine-readable graphics, and in such an arrangement the hologram is preferably attached to the substrate in such a way that it is difficult to remove without destroying the hologram (to inhibit attaching the hologram to a substrate with counterfeit data).

One way of linking data in the hologram and in the chip is simply to store an electronic or soft copy of the hologram on the chip. This is facilitated by recording a hologram of an electronically reproduced biometric image which is substantially planar. This facilitates storage of a two-dimensional rather than three-dimensional image on the chip, occupying less storage space, and also speeds up comparison of the holographic and electronically stored images. Preferably, in such an arrangement, the stored image is substantially the same as the original image used to create the hologram, further facilitating comparison of the two images.

In another arrangement a key is embedded in the hologram as additional data (in addition to the image) and data stored on the chip is encrypted with this key. This key may comprise, for example, a key of a public key infrastructure (PKI) technology. This then links the holographic image (which, because it is a biometric image, may be used for identification purposes) to the data stored on the chip (because, for example, it is difficult to re-write just part of the data stored on a chip when encrypted or signed in this way).

In a related aspect the invention provides a method of verifying data stored on a data carrier, the data carrier comprising a hologram storing data to reproduce an image of a portion of a human body characteristic of an individual; and a second data bearing

device; and wherein data stored by said second data bearing device is verifiable using data stored in said hologram, the method comprising: reproducing said characteristic image: comparing said reproduced image with a view of an individual to verify data stored in said hologram; verifying, responsive to a result of said comparison, data stored by said second data bearing device using data stored in said hologram.

The verifying is preferably performed automatically, by machine, and may comprise comparing and/or decrypting, and may employ the stored image data or additional data stored in the hologram in association with the image data. The method provides improved data verification because, among other reasons, holograms are difficult to copy or reproduce; this is especially true of volume holograms. The comparison of the reproduced image from the hologram with the view of an individual may be performed visually but may also be performed by machine, for example automatically capturing image data of the view and comparing this with an electronically captured image of the reproduced image read from the hologram.

In a simpler arrangement an image from the hologram, say of a fingerprint, and an electronically captured image of the fingerprint of the individual may be compared by eye, although preferably in this example conventional methods of fingerprint comparison are employed such as the co-incident sequence method (a standard technique employed by police forces for many decades). A second view of the hologram, preferably separable from the first image by the viewing system, contains a code derived from the fingerprint image and, optionally, from personal details of the relevant individual. This code may also be stored as graphics on the card and/or on a magnetic strip and/or in a chip.

In a further aspect the invention provides apparatus for capturing and recording a biometric image as a hologram for a data carrier, the apparatus comprising: a biometric image capture device; means for electronically reproducing said captured image as a reproduced image; and means for recording said reproduced image in a holographic recording material for developing into a hologram.

Electronically reproducing the captured image provides control over the image and facilitates subsequent verification operations as described above. In preferred embodiments the electronically reproduced image is substantially planar. The apparatus may also include means to write additional data, such as a code, into the hologram; this additional data may be captured, for example, at a user input terminal or downloaded from a database over a network. In some preferred arrangements the apparatus also includes means for storing the captured image in a data store for comparison with the recorded image. The data store may comprise a remote data store, accessed, for example, when data is written into a chip for creating a data carrier, or data may be written directly into a chip on a card or other substrate. Preferably this chip is then kept securely in association with the hologram until the hologram has been chemically processed or developed to render it substantially permanent.

In a further aspect the invention provides apparatus for capturing and recording a biometric image comprising a biometric image capture device, a spatial light modulator to reproduce a substantially two-dimensional version of the captured image, and a holographic writer to write the reproduced image into a hologram. Preferably the image is written as a reflection hologram. Preferably the spatial light modulator is in close proximity to or adjacent the holographic recording medium; preferably a diffuser is employed in the object (or reference) beam to create a hologram with a diffused or speckled appearance rather than a hologram with a specular appearance.

In a further aspect the invention provides a method for creating a data carrier incorporating a hologram and a second data bearing device, the method comprising capturing biometric information and using this to create a (preferably substantially two-dimensional) image; recording the image into a hologram; and recording data derived from or verifiable using data stored in the hologram on a semi-conductor memory device. Thus preferably the memory device stores a version of the image, for example a compressed version of the image, and preferably the memory device also stores cryptographic data which is also written into the hologram. Preferably the data is stored as a reflective hologram. Preferably the memory device and hologram are bonded to a common substrate or otherwise encapsulated in an identity document or identifying card.

The invention further provides processor control code, in particular on a data carrier such as memory, a disk or an optical or electrical signal carrier, to implement the above described method.

Further aspects of embodiments of a system and data carrier for the capture and recording of a biometric image, in particular a fingerprint, as a hologram for use with a document such as an identity card are described below.

1. The biometric, in particular fingerprint, image is preferably captured by a reader and reproduced on a substantially planar spatial light modulator (LCD display) for recording as a hologram. This solves a number of problems with the arrangements described in the prior art and, in particular, provides a substantially planar hologram which simplifies image comparison and recognition. This further provides advantages such as enhanced viewing angle, as well as facilitating the use of other recording techniques as described below (e.g. mechanical contact with film). Furthermore this allows the image of the fingerprint to be positioned in a plane such that only a camera correctly focused onto the plane will see a correctly focused image from the hologram. Further by recording an image in a plane the options of using additional, for example, substantially parallel planes to record additional information, such as bibliographic and other details, is made available.

2. The holographic image is recorded as a volume, reflection hologram in which, roughly speaking, the fringes are in planes substantially parallel to the surface of the hologram rather than substantially perpendicular to the surface. Volume holograms have special advantages, and in particular they difficult to copy.

3. Any conventional holographic recording material may be employed but preferably the hologram is recorded in silver halide rather than photopolymer film, which facilitates rapid recording of a hologram and hence makes rapid creation of biometric holograms on a large scale practically feasible using bench-top apparatus. This could, for example, be installed in secure locations

such as, say, larger post offices. Furthermore the use of silver halide film with small silver particles enables the holograms to be fabricated so as to be substantially transparent, thus enabling a hologram to overlie other information on a document, for example, text.

4. The recording apparatus preferably utilises a spatial light modulator (LCD display) which is preferably in mechanical contact with the holographic film (for example, separated by a small distance by means of a glass or quartz substantially index-matching spacer). This stabilises the mechanical arrangements for recording the image, again facilitating bench-top operation.

5. The SLM (spatial light modulator) image may be substantially in contact with the film (giving a large, potentially up to 180°, viewing angle) or the image may be spaced away from the surface of the recording film by a distance of 0 to 1 cm (and less than the coherence length of the recording laser). This positions the holographic image a corresponding distance from the surface of the recorded holographic film enabling the advantages referred to above regarding image planes. By employing a small, controlled (or controllable) distance, the viewing angle may still be kept large. Furthermore a diode laser with only a short coherence length may then be employed, giving a cost saving.

6. The underside of the SLM may be provided with a diffuser (so that the illuminating laser illuminates the SLM through the diffuser, which is preferably adjacent the SLM) since this creates a preferred form of hologram. Such a hologram has a matt or transparent rather than shiny surface and having, under laser illumination, a speckle pattern characteristic of a genuine hologram.

7. Preferably the bench-top recording apparatus includes storage and/or network communication means for recording a "golden" image of the captured biometric image (fingerprint) which exactly corresponds to the image displayed by the SLM, again considerably simplifying rapid comparison of a recorded fingerprint hologram (or other biometric image) for identification purposes. Preferably this image is stored on the above described data carrier; it may be signed or

encrypted, for example verifiable and/or readable using a key embedded in the hologram. Because the hologram records not the biometric image per se but rather a captured and re-displayed electronic representation of the biotmetric image the golden image can, in effect, be an exact copy of the recorded hologram thus facilitating, say, a pixel-by-pixel comparison of a holographically recorded image with a stored image rather than having to rely on much slower, more costly and computationally expensive image processing techniques for biometric image (e.g. finger or face) recognition, which in general are still not well developed.

These and other aspects of the invention will now be further described, by way of example only, with reference to the accompanying figures in which:

Figures 1a and 1b show, respectively, a data carrier incorporating a biometric hologram according to an embodiment of the present invention, and a flow diagram for the fabrication of the data carrier of figure 1a;

Figures 2a and 2b show, respectively, a biometric hologram writer, and a data carrier fabrication process;

Figure 3 shows a computer control system for the apparatus of figure 2a;

Figures 4a to 4c show details of a holographic writer and first and second alternative holographic film supports; and

Figure 5 shows a schematic diagram of an optical arrangement for the apparatus of figure 2b.

Referring to figure 1a, a data carrier 10 comprises an integrated circuit memory chip 12, either having contacts (as shown) or for contact-less communication with a reader. The data carrier 10 also includes a hologram 14 storing biometric and other data and text 16 such as a name, address, national security number and the like. Data carrier 10 may be

based upon a so-called smartcard and may comprise an identity card or document, driving licence, passport, credit card or any other form of identification.

Referring to figure 1b card 10 is created by capturing biometric information such as a fingerprint (step 20) and creating a high resolution two dimensional image from this (step 22). Where necessary relevant biometric data is extracted (step 24) for storage on the chip 12. In the case of a fingerprint, for example, data stored may comprise five-zone coincidence sequences, eight or nine coincidences generally being taken as sufficient for a match. Optionally other data may be created or input for storage with the hologram. At step 26 cryptographic data is created, for example a key, and this is combined with the biometric image and presented for storage as a reflective or reflection hologram (step 28); the biometric data or image together with any additional data, preferably encrypted with the key or another key of a pair to which the key belongs is stored on the integrated circuit memory device 12 (step 30). The chip and hologram are then encapsulated in an identity document (step 32).

Figure 2a shows a holographic recording system. Data for recording with the hologram may be entered into the terminal (which may also create or download random numbers for keys), and write once read many (WORM) records are created locally and also, via a network, at a remote database. The local and/or remote records may also include a 'golden' image corresponding to a captured image as reproduced by an electronic reproduction system for recordal as a hologram.

The film is held securely within the hologram writer, for example accessed by a mechanical key, and a secure film box can be removed from the writer and sent securely for chemical processing. A typical process for incorporating the developed holographic film and other data (ie the semi conductor chip) into a document is outlined in figure 2b.

Referring next to figure 3, this shows a block diagram of a computer control system for the apparatus of figure 2a. Biometric data such as a fingerprint image is captured by commercial off the shelf equipment such as the BAC Securetouch USB2000 available from Bannerbridge plc of Basildon, UK and provided to an image pre-processor 302 which, under control of a control processor 304, provides an image to display driver 306

for display on an LCD display 308, for example at SVGA resolution, at a size of approximately 30mm^2. The size and resolution of the display may be determined based upon processing power and cost. The LCD display acts as a spatial light modulator as described below with reference to figure 4a and thus preferably allows illumination through the device. Typically such a display comprises a micrometer thick sheet of polarising material followed by electrically configurable liquid crystal material. The LCD display may be of a type which has permanently on or off pixels rather than pixels which are refreshed, for example a ferroelectric liquid crystal device so that the pixels stay in either an on or an off (black or white) state for the duration of the image recordal, typically around two seconds. Alternatively a conventional, raster scanned display may be employed, thus facilitating recordal of grey levels, useful, for example, for representing faces. It will be appreciated that the recorded biometric image is a monochrome image and, where necessary, a captured input image is converted into a monochrome image by preprocessor 302. A suitable LCD display is available from Central Research Laboratories Ltd of London, UK, for example model SVGA2 monochrome transmission LCD. An LCD display without an in-built polariser may be employed with plane polarised laser illumination, which in effect provides approximately 50% more light.

Referring next to figure 4a this shows the optical configuration of the spatial light modulator and film. The spatial light modulator may be substantially adjacent the film or may be spaced apart from the film by a glass or quartz spacer. Spacers of 2, 4 or 6mm may be employed, optionally mechanically selectable on the control of the computer controller 304 in order to record images at different planes within the hologram. The maximum spacing between the spatial light modulator and film is determined by the coherence length of the laser, and is typically around 80mm for a diode laser (since, as shown later in figure 5, optical path lengths from the laser for the object and reference beams are preferably substantially matched).

Preferably the arrangement includes a diffuser prior to the spatial light modulator comprising, for example, ground glass or bi-refringent plastic material such as polycarbonate or polyester film. Such diffusers are available from Lee Filters in the UK. The diffuser does not destroy the hologram since the differences in optical path

lengths to the film from diffused rays originating from a point on the diffuser is very small, but the diffuser has the effect of providing a hologram with a speckle pattern rather than a so-called shadowgram which appears shiny like a mirror.

Many mechanical schemes may be employed for holding the film in close proximity to the spatial light modulator or spacer depending, for example, on whether sheet fed or roll fed film is employed. Figures 4b and 4c show two examples of film transport mechanisms; for sheet film a sheet feeder may be employed; optionally a vacuum chuck may also be used to ensure the holographic recording material bears against the spatial light modulator or spacer. In a less preferred arrangement a mounting frame holds the SLM and/or spacer in a fixed or controllable spatial relationship with respect to the film. In all the above arrangements index matching adhesive may be employed if necessary.

Figure 5 shows one example of an optical configuration for the apparatus of figure 2a. In particular this optical configuration shows how the reference beam may be tilted between two alternative positions in order to record two sets of data within the holographic film, for example viewable at different wavelengths or in different planes (with reference to the plane of the recording material) of the generated holographic image.

No doubt many other effective alternatives will occur to the skilled person and it will be understood that the invention is not limited to the described embodiments but encompasses modifications apparent to those skilled in the art within the spirit and scope of the claims appended hereto.

CLAIMS:

1. A data carrier comprising:

a hologram storing data to reproduce an image of a portion of a human body characteristic of an individual; and

a second data bearing device; and

wherein data stored by said second data bearing device is verifiable using data stored in said hologram.

2. A data carrier as claimed in claim 1 wherein said data stored by said second data bearing device comprises first and second data, said first data being for verification of one of said first data and said image with the other, and second data being verified by said verification.

3. A data carrier as claimed in claim 1 or 2 wherein said hologram stores additional data, and wherein said data stored by said second data bearing device comprises third and fourth data, said third data being for verification of one of said additional data and said third data with the other, and fourth data being verified by said verification.

4. A data carrier as claimed in claim 1, 2 or 3 wherein said image comprises a substantially two-dimensional image.

5. A data carrier as claimed in any preceding claim wherein said hologram comprises a volume reflection hologram.

6. A data carrier as claimed in any preceding claim wherein said second data bearing device comprises an integrated circuit memory device.

7. A method of verifying data stored on a data carrier, the data carrier comprising

a hologram storing data to reproduce an image of a portion of a human body characteristic of an individual; and

a second data bearing device; and

wherein data stored by said second data bearing device is verifiable using data stored in said hologram, the method comprising:

reproducing said characteristic image:

comparing said reproduced image with a view of an individual to verify data stored in said hologram;

verifying, responsive to a result of said comparison, data stored by said second data bearing device using data stored in said hologram.

8. Apparatus for capturing and recording a biometric image as a hologram for a data carrier, the apparatus comprising:

a biometric image capture device;

means for electronically reproducing said captured image as a reproduced image; and

means for recording said reproduced image in a holographic recording material for developing into a hologram.

9. Apparatus as claimed in claim 8 wherein said reproduced image is substantially planar.

10. Apparatus as claimed in claim 9 comprising means to record for said hologram a first view comprising said reproduced image and a second view comprising additional data.

11. Apparatus as claimed in claim 9 or 10 wherein said hologram comprises a volume or reflective hologram.

12. Apparatus as claimed in any one of claims 8 to 11 further comprising means for storing said captured image in a data store for comparison with said recorded image.

ABSTRACT:

Data Verification Methods and Apparatus

This invention generally relates to methods and apparatus for verifying data, and more particularly to holographic data carriers and apparatus for creating such data carriers, and to methods of verifying data stored on holographic data carriers.

A data carrier comprising: a hologram storing data to reproduce an image of a portion of a human body characteristic of an individual; and a second data bearing device; and wherein data stored by said second data bearing device is verifiable using data stored in said hologram.

Figure 2a

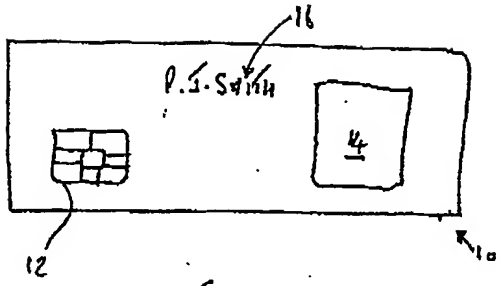


FIGURE 1A

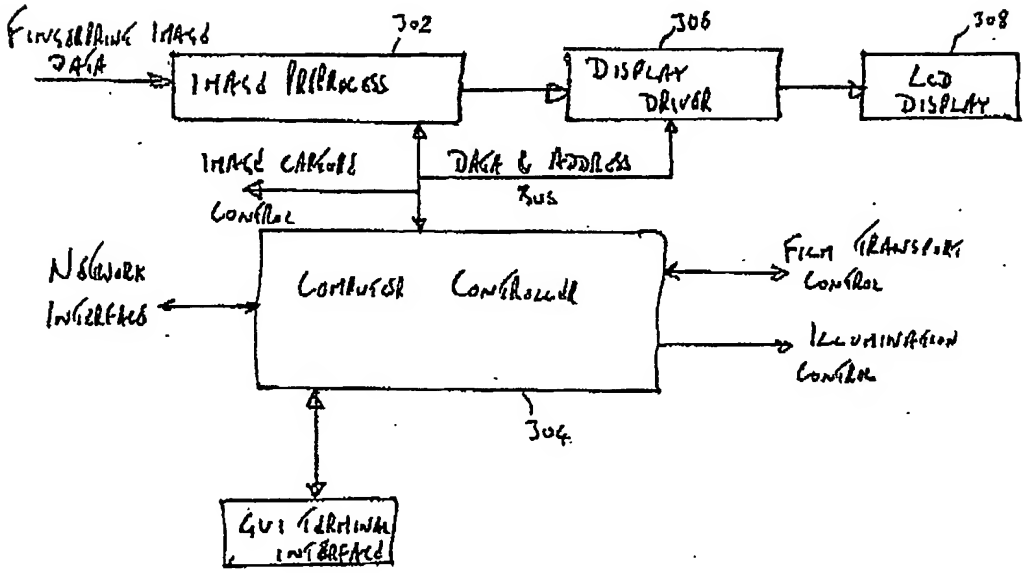


FIGURE 3

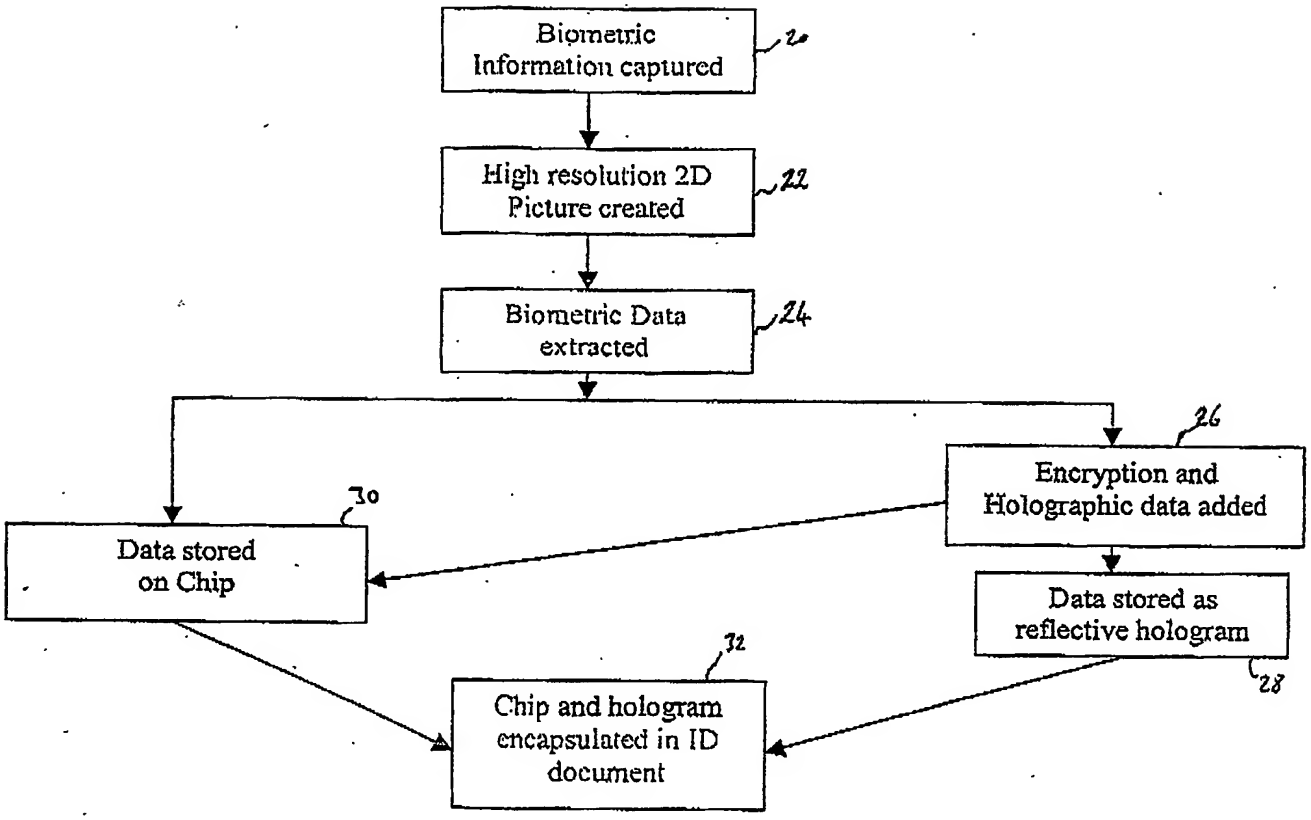

Biometric Information captured
20
High resolution 2D Picture created
22
Biometric Data extracted
24
26
Encryption and Holographic data added
30
Data stored on Chip
Data stored as reflective hologram
28
32
Chip and hologram encapsulated in ID document

Figure 1a

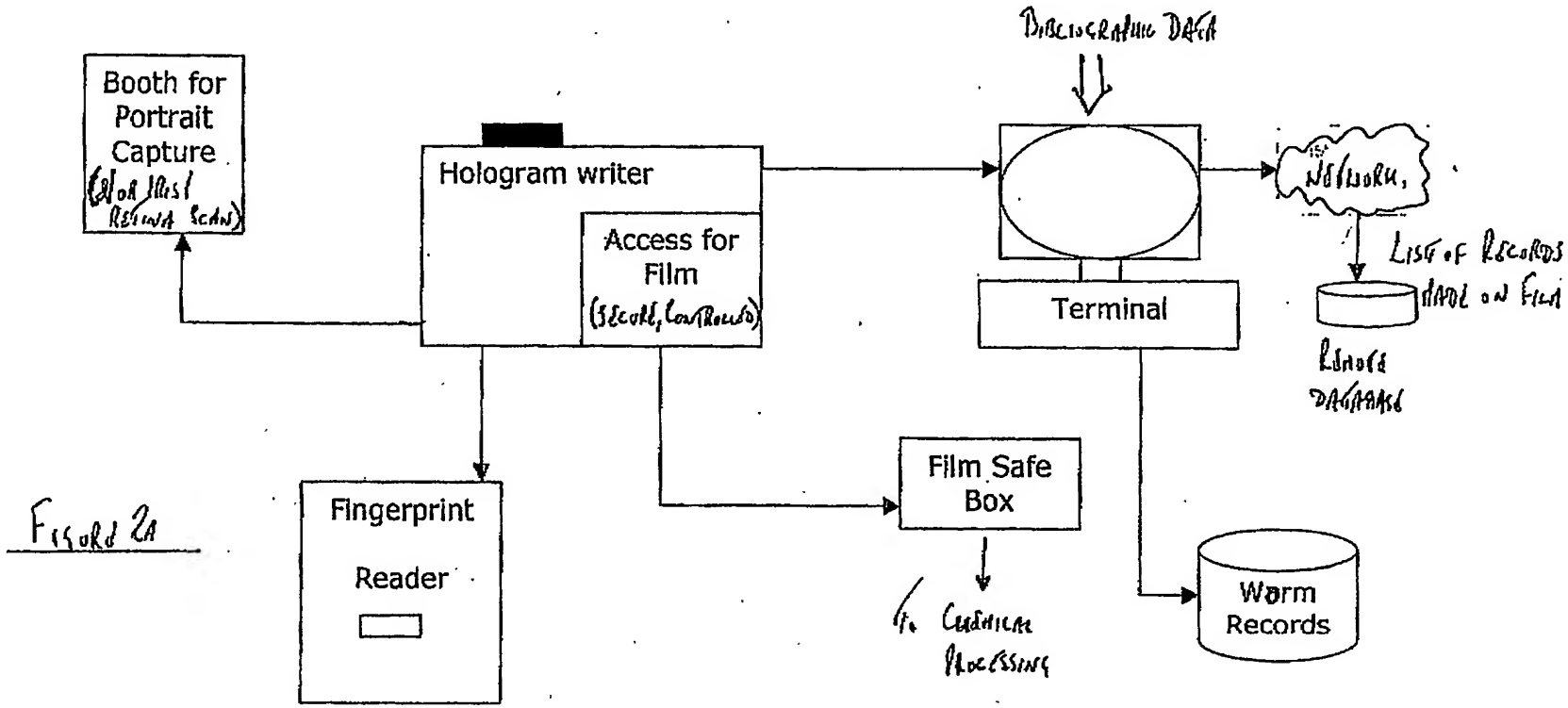


Figure 2A

Figure 2B

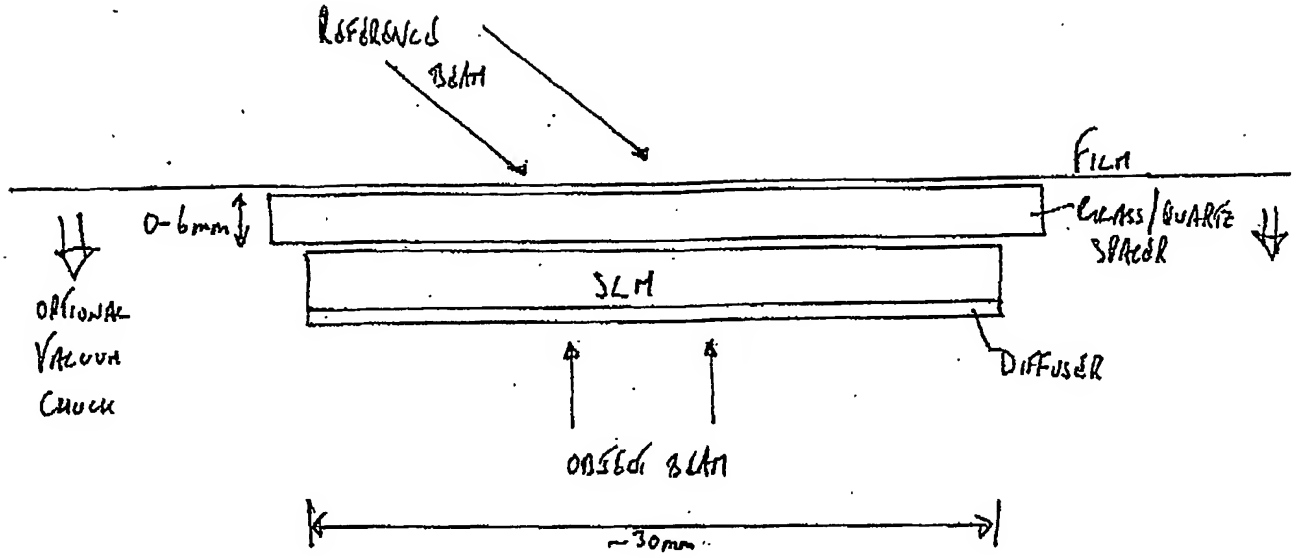


FIG. 4A

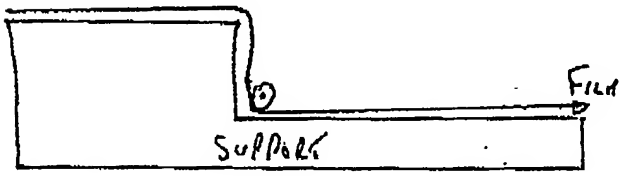


FIG 4B

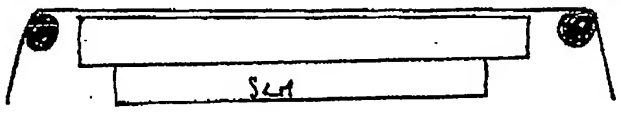


FIG. 4C

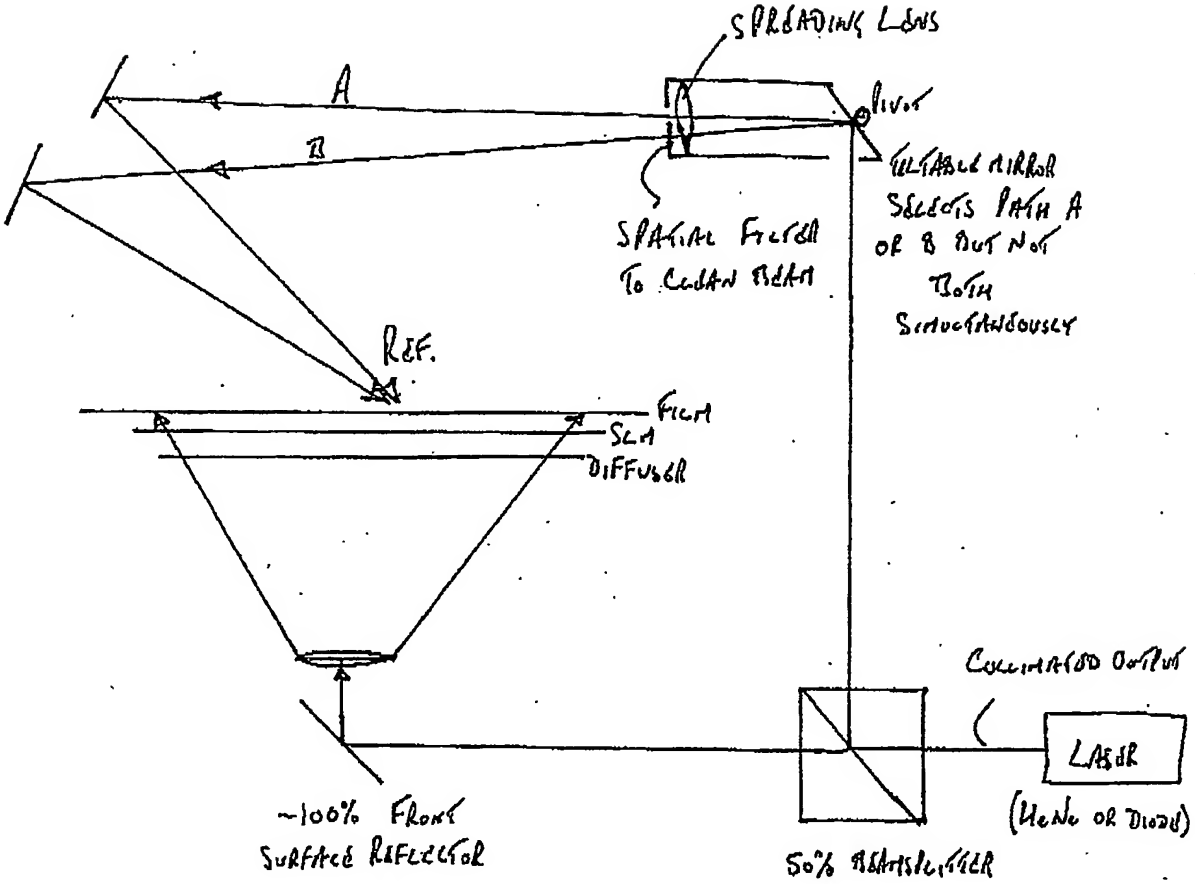

SPREADING LENS
A
B
MIRROR
STEERABLE MIRROR
SELECTS PATH A
OR B BUT NOT
BOTH
SIMULTANEOUSLY
SPATIAL FILTER
TO CLEAN BEAM
REF.
FILM
SLM
DIFFUSER
COLLIMATED OUTPUT
LASER
(HeNe OR DIODE)
~100% FRONT
SURFACE REFLECTOR
50% BEAMSPLITTER

FIGURE 5